Manual de Seguridad en Cibernética

www.NJConsumerAffairs.gov ■ 1-888-656-6225

Seguridad *en* Cibernética

Introducción

Una guía de protección para el consumidor en el mundo cibernético

Estimado Consumidor de Nueva Jersey:

"Cybersecurity" (Seguridad en la Cibernética) se refiere a la protección de todo lo que puede estar conectado con el internet: computadoras, teléfonos inteligentes, sistemas de comunicación; nuestra información personal; nuestra privacidad; y nuestros hijos.

El internet es un instrumento extremadamente útil y versátil que se ha convertido en una herramienta indispensable para el trabajo, la educación, el entretenimiento personal y para conectarnos con la familia y los amigos. Si se usa de una manera responsable, y tenemos cuidado de protegernos y proteger nuestra información, el internet continuará siendo un recurso indiscutiblemente valioso.

Este manual cubre tres tópicos: **"Virus, *Phishing*, y Robo de Identidad", "Anuncios, Aplicaciones y su Seguridad Personal",** y **"Predadores y Acoso Cibernético".**

Aunque la básica información acerca de la protección personal es siempre la misma, ciertas cosas pueden cambiar porque el internet está constantemente cambiando. Por esta razón, el manual termina con una lista de recursos en línea para que el consumidor obtenga información actualizada.

Póngase en contacto con nosotros si sospecha fraude o si ha sido una víctima de éste. Recuerde que la División es la agencia de protección para el consumidor.

Atentamente,

La División de Asuntos del Consumidor de Nueva Jersey

Índice

Capítulo 1: ***VIRUS, PHISHING, Y ROBO DE IDENTIDAD***

El problema: Artimañas tecnológicas y sicológicas 5
La solución: Erija sus defensas 10

Capítulo 2: ***ANUNCIOS, APLICACIONES Y SEGURIDAD PERSONAL***

El problema: Confusas, engañosas o falta de políticas de privacidad..... 19
La solución: Tome control de su privacidad..... 28

Capítulo 3: ***PREDADORES Y ACOSO CEBERNÉTICO***

El problema: Depravadores, acosadores y contenido inapropiado..... 33
La solución: Comuníquese con su familia y empodérese..... 39

Índice

APÉNDICE I: SI HA SIDO VÍCTIMA DE ROBO DE IDENTIDAD 44

APÉNDICE II: RECURSOS ADICIONALES 48

Notas 49

Sea un consumidor bien informado.... ¡Podemos ayudarle!

Seguridad *en* Cibernética

CAPÍTULO PRIMERO

Una guía de protección para el consumidor en el mundo cibernético

El problema: Artimañas tecnológicas y sicológicas **-El robo de identidad**

El robo de identidad es el crimen financiero que está creciendo con más rapidez. Ocurre cuando un ladrón asume la identidad de una víctima para poder aplicar por tarjetas de crédito, préstamos, u otros beneficios, y usa esa información para acceder a las cuentas de banco de ésta. El ladrón maximiza el crédito de la víctima, le quita el dinero del banco, y luego se va en pos de otra nueva.

La víctima de robo de identidad termina con miles de dólares en deudas, con el crédito arruinado y con la cuenta de banco vacía. Hasta que la víctima pueda aclarar lo que le ha pasado, será difícil para ésta encontrar trabajo, comprar o arrendar un auto o casa, obtener un préstamo, o realizar cualquier otra actividad si necesita un antecedente de crédito.

Los ladrones pueden robar su identidad a través de ***phishing***, en la que los criminales engañan a las víctimas para obtener información personal, la contraseña de internet, el número de seguro social, o el de la tarjeta de crédito; la roban invadiendo su computadora con spyware que lee su información personal; o simplemente robándole la cartera.

Nota: *Para información en lo que debe hacer* ***si ha sido víctima de robo de identidad****, vaya al Apéndice I de este manual, a la página 46.*

Las muchas formas de *malware*

"Malware" son "programas dañinos" que están diseñados para invadir y trastocar la computadora de las víctimas. *Malware* se puede usar para eliminar y destruir información importante; reducir la velocidad de la computadora hasta que llegue a un paro total; o para espiar y robar información personal.

Las más conocidas clases de ***malware*** son los ***virus*** y los ***worms***, que infectan a las computadoras, se replican, y se extienden a otras computadoras. Se pueden transmitir vía email, o a través de redes. Otra clase de ***malware*** es el ***caballo de Troya***. Igual que el caballo de Troya de la leyenda griega, parece un regalo- pero cuando pulsa en él, descarga un enemigo escondido.

Spyware, como se ha mencionado antes, colecciona su información personal como número de tarjeta de crédito o de cuenta bancaria sin que lo sepa. Otras veces ***Spyware*** puede dirigir su navegador a ciertas redes, mandarle anuncios instantáneos *(pop-up ads)*, y cambiar la configuración de su computadora.

***Phising* e ingeniería social**

Kevin Mitnick, previamente famoso por ser un criminal de computadoras, ahora un consejero de seguridad de informática, en una entrevista con la revista Times el 11 de Agosto del 2011, dijo que los criminales usan artimañas sicológicas con la habilidad de diseñar ***malware*** –para crear una combinación conocida como ***ingeniería social***.

Él dijo que un ***hacker*** (pirata de informática) aprende lo que a usted le gusta y no le gusta por lo que pone en Facebook. "Si yo sé que a usted le gusta ***Angry Birds*** (un juego popular de teléfono inteligente), puedo mandarle un email pretendiendo que viene de ***Angry Birds*** con una versión nueva. Una vez que lo descarga, yo tendré acceso completo a su teléfono," dijo Mitnik.

Ataques como estos son una forma de ***phishing***. A través de ***phishing*** e ***ingeniería social***, los piratas de informática engañan a las víctimas a que den información sensitiva- o a que descarguen ***malware***-sin que éstas lo piensen dos veces.

Ingeniería social puede tener la forma de emails o mensajes instantáneos que parecen que vienen de una fuente fiable. Estos emails fraudulentos se asemejan a los de su banco, su sitio

de compras, un amigo o incluso el gobierno. El mensaje puede contener enlaces a una versión falsa de un sitio web de una compañía, completo con gráficas y el logotipo de la corporación.

Un mensaje ***phishing***, le puede pedir que pulse en un enlace o web fraudulentos que demandan su información personal o financiera – y usted termina dándosela a un ladrón de robo de identidad. O puede recibir un email con un anexo que contiene un virus. Si abre el anexo, puede descargar un **caballo de Troya** y el estafador tendrá completo acceso a su computadora.

Un ejemplo de una estafa ***phishing***: en Marzo del 2012 consumidores, algunos de ellos de sitios tan lejanos como Baltimore, empezaron a llamar al Estado de Nueva Jersey, diciendo que habían recibido una carta de 11 páginas que parecía oficial, y que decía que venía del Fiscal General de Nueva Jersey. La falsa carta invitaba a los consumidores a aplicar por su parte a un acuerdo legal (ficticio) de múltiples millones. Ésta incluso contenía un número de teléfono y una dirección de correo electrónico manejada por el perpetrador de la estafa. Si alguien llamaba, un estafador contestaba la llamada pretendiendo ser un empleado del Estado y les pedía a las víctimas que mandaran su número de seguro social y otra información personal. A esta estafa se le dio el nombre de ***"Impostor de Fiscal General".***

El New New Internet, una web de noticias de seguridad en cibernética, ha anotado que los ***hackers*** lanzan estafas ***phishing*** a través de mensajes instantáneos, **Facebook, Twitter,** y otros sitios webs de redes sociales. En una de estas estafas, los usuarios de **Facebook** encontraron un enlace a un video falso que tenía una miniatura de una joven en bikini con el título "distráete con chicas en bikinis". El correo parecía que venía de los amigos del usuario. Otra semejante usó correos con el título "muérete de risa", el cual parecía ser un sitio web de humor. En ambos casos, los enlaces intentaban instalar ***malware*** en las computadoras de los usuarios.

Una amenaza de crecimiento exponencial

The Wall Street Journal reportó en Mayo del 2011 que "uno de cada 14 descargos del internet es un programa de ***malware***". **Secure Works**, un proveedor de servicio de protección de información, reportó en el 2010 que los EE.UU. es "el país que tiene menos protección en cibernética en el mundo", con 1.66 ataques por computadora durante el año anterior –comparado a solamente 0.1 ataques por computadoras en Inglaterra. **Symantec**, un fabricante de programas de seguridad para el internet, reportó en el 2008 que pronto nueva ***malware*** sobrepasará a los nuevos programas legítimos de ***software***.

De los 140 billones de emails mandados cada día, el 90 por ciento son anuncios no deseados o correos electrónicos basura, según un reporte en el 2010 en **The Economist**; de esos, cerca de un 16 por ciento son estafas de ***phishing***. Es más fácil que nunca para los estafadores crear emails personalizados que parecen legítimos y atraer a víctimas que terminan abriéndolos - y esto es porque hay más información que nunca acerca de individuos. Considere la cantidad de información que hay en línea acerca de usted debido a sitios de socialización, sitios web de su trabajo, documentos del gobierno y otras fuentes incluyendo sus cuentas de servicios públicos.

La solución: Erija sus defensas-Las siguientes sugerencias están adaptadas del **United States Computer Emergency Readiness Team o US-CERT** (Equipo de Preparación de Emergencia de Informática de los Estados Unidos), dentro del **U.S. Department of Homeland Security** (Departamento de Seguridad Nacional de Estados Unidos) Para más información vaya a: **www.US-CERT.gov**

Herramientas de protección

Use y mantenga programas de buena reputación de *antivirus.* *Programas de antivirus buenos reconocen y protegen a su computadora en contra de los virus más comunes. (Puede chequear en línea los comentarios de la gente para ver que versiones están disponibles). Una vez que ha instalado un paquete antivirus, de vez en cuando, úselo para escanear su computadora por completo. Encuentre un paquete que incluya herramientas de* ***antispyware****.*

Mantenga su programa de *antivirus* actualizado. Instale parches de ***software*** y de seguridad actualizados en su antivirus de software regularmente. Les ayudarán a proteger su computadora en contra de nuevas amenazas al mismo tiempo que se descubren. Muchos vendedores y sistemas de operación ofrecen actualización automática. Si esta opción está disponible, puede utilizarla.

Instale o permita un *firewall* (cortafuegos). Los cortafuegos lo protegen de ataques externos a su computadora o red de maligno o innecesario tráfico de internet. Son especialmente útiles para los usuarios que siempre están conectados a cable o al ***módem*** **Digital Subscriber Line.** Algunos sistemas de operación incluyen un cortafuego; si el suyo tiene uno asegúrese que

está funcionando. Si no, considere comprar ***hardware*** o ***software*** que tenga uno.

Use herramientas de *antispyware*. La mayoría de los paquetes de software de antivirus están vendidos con herramientas de antispyware. ***Nota:*** Muchos vendedores producen software antivirus. Decidir cuál escoger puede ser confuso. Todo el ***software*** esencialmente preforma la misma función, así que pregunte por recomendaciones, acerca del precio, características y disponibilidad.

No es una buena idea instalar muchas clases de *software* de seguridad. Demasiados programas de seguridad pueden afectar el rendimiento de la computadora y la eficacia del mismo ***software***.

Finalmente, **tenga cuidado con emails que no ha solicitado y anuncios instantáneos** que dicen que contienen antivirus. No pulse en ellos o los abra. Por lo general son ***Trojan horses***, listos para infectar su computadora..

Chequee las configuraciones de privacidad y seguridad de su navegador de red. Casi todas las computadoras y los teléfonos inteligentes vienen con uno o más navegadores

instalados (tales como **Safari, Firefox, Internet Explorer, Chrome** u otros). Estos navegadores tienen predeterminadas configuraciones que hacen un balance entre mantener su computadora segura y permitir la funcionalidad que espera de la mayoría de los sitios webs.

Las configuraciones crean límites en la medida que la computadora permitirá a aplicaciones del internet –como ***cookies***, **Active X y Java**-que ayudan a la red preformar funciones importantes. Por ejemplo, pueden rastrear que es lo que hay en su "carrito de compra" o recordar su contraseña para iniciar una sesión para que no tenga que reentrarla cada vez.

Si su navegador permite interacción sin límite con los ***cookies*** que rastrean toda la actividad de su computadora, usted puede estar a mayor riesgo de un ataque de ***malware*** –o de ser solicitado por **anuncios de *software*** (más acerca de esto en el capítulo siguiente). **Pero si bloquea estas aplicaciones completamente, los sitios web no pueden funcionar eficazmente.**

Encuentre el balance que funcione para usted. Chequee la privacidad y las configuraciones de privacidad de todos los navegadores que están instalados en su computadora, y ajústelos como sean necesarios.

Para información específica, en un navegador especial, visite el sitio web del vendedor (por ejemplo, visite el sitio web de Microsoft Windows para aprender cómo ajustar las configuraciones de **Internet Explorer**; o el sitio **Apple** para aprender acerca del navegador **Safari**). Si el vendedor no provee información acerca de cómo asegurar un navegador, póngase en contacto con ellos y pida la información.

Si usa un enrutador inalámbrico. Sistemas de enrutadores inalámbricos emiten su conexión de internet a través de una señal de radio a las computadoras. Si no asegura apropiadamente esta conexión puede exponer su conexión de internet a otros usuarios, y causarle posibles problemas.

Lea el manual de su enrutador de información para saber cómo: esconder su red inalámbrica (a veces llamado creando una "red cerrada"); renombrar su red (cambie el determinado **"identificador de grupo de servicio"** o **"extendido identificador de grupo de servicio"** a una denominación que los piratas de informática no lo puedan adivinar); poner su red inalámbrica en contraseña (convierta el tráfico entre su computadora y su ruta en código); y cambiar la contraseña de su administrador.

Además, refiérase al manual del usuario para deshabilitar la opción de compartir un registro en su computadora (a no ser que necesita compartir el directorio y los registros de su red, en cuyo caso debe proteger todo lo que comparte con una contraseña). **Mantenga sus parches de *software* inalámbricos y actualícelos,** periódicamente chequeando el sitio web del fabricante para cosas nuevas. Además es una buena idea aprender si su **Internet Service Provider** o **ISP** (Proveedor de Servicio de Internet) ofrece opciones de seguridad inalámbrica.

Use contraseñas inteligentes. No use contraseñas que están basadas en información personal que un pirata de cibernética lo puede adivinar fácilmente; y no use palabras que se pueden encontrar en un diccionario. Un método para crear contraseñas es basarse en una serie de palabras y **técnicas de memoria o mnemotécnica,** que le puede ayudar a recordarlas o descifrarlas. **US-CERT** da este ejemplo: en vez de usar la palabra "portero" puede usar **"MgSpdf"** por **[M]e [g]ustaría [S]er [p]ortero [d]e [f]utbol.** Mezclando las letras mayúsculas con las minúsculas sirve como una distracción, así como añadir, números y caracteres. Cambie el ejemplo a: **"1MgSpdf!"** y vea como parece más complicado una vez que ha añadido números y caracteres.

No dejen que lo 'pesquen'

Nunca se fie de un email, mensaje de texto, ventana instantánea, mensaje de Facebook, etc. *-que no ha solicitado- que le pida: su número de Seguro Social, cuenta de banco, que pulse en un enlace, abra un anexo, o que mande dinero.*
No se fie del mensaje aunque parezca muy convincente; incluso si parece que viene de su banco, del gobierno, de su ISP, o de su mejor amigo.

Siempre verifique la autenticidad del mensaje antes de responder. No use la dirección del correo electrónico, el enlace, o número de teléfono del mensaje. Si cree que es de compañías con la que hace negocio, busque la página web de éstas y comuníquese con ellas.

En Junio del 2012, el Better Business Bureau (Buró de Mejores Negocios) dijo que ciertos consumidores recibieron, por toda la nación, falsos emails que eran casi idénticos a los emails de alerta que Verizon manda a sus clientes recordándoles el pago mensual. Los emails incluían un enlace que decía: "Mire y pague su cuenta"- un enlace que llevó a las víctimas a un sitio fraudulento. En vez de seguir los enlaces, los consumidores podrían haber verificado

independientemente si el mensaje era verdadero yendo al sitio web de Verizon y haberse puesto en contacto con el servicio para el cliente.

Use sentido común. Nunca abra anexos de emails a no ser que sepa quién los mandó. Nunca abra programas si no sabe de dónde vienen. Nunca pulse en un enlace de un anuncio instantáneo. Tenga cuidado con ***software*** que dice que la puede descargar gratis, o emails que ofrecen programas de ***antimalware.***

No se fie de los CD de fabricación casera, o disquetes *(floppy disks)* y los *flash drives.* Si los va a usar en su computadora, escanéelos con su ***software*** de antivirus antes de usarlos.

Qué hacer si su computadora se "contamina" Lo primero desconecte su computadora del Internet. Esto previene que la ***malware*** transmita su información a un agresor. Luego, intente remover el código maligno. Si tiene anti virus ***software*** instalado en su computadora, actualice las definiciones de los virus (si puede) y escanee su sistema por completo. Si no tiene antivirus ***software,*** usted puede comprarlo en una tienda local de computadoras.

Si el *software* no puede remover la infección, lleve la computadora a una compañía

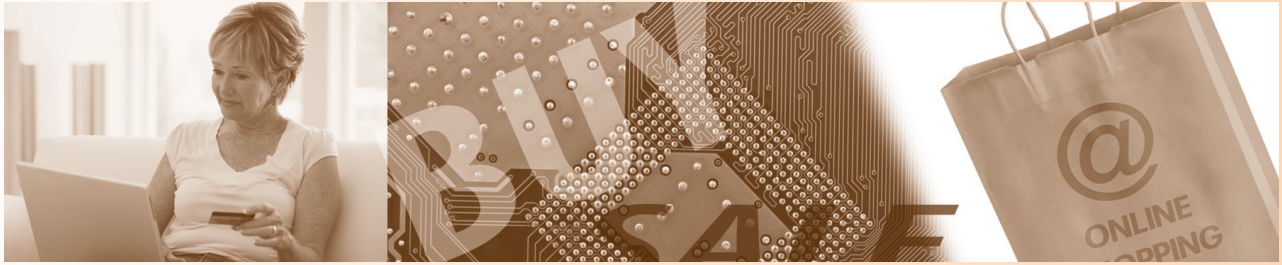
de ayuda tecnológica para resolver el problema. Como con cualquier compra, puede hacer una indagación para encontrar una compañía en línea de buena reputación y lea los comentarios en línea acerca de ella, y póngase en contacto con la **División de Asuntos del Consumidor** para saber si se han puesto quejas en contra de ésta antes de usarla.

US-CERT anota que como último recurso, usted puede reinstalar su sistema de operación, generalmente con un disquete de restauración de sistema que con frecuencia viene con las nuevas computadoras. Tenga cuidado porque este disquete puede borrar todo lo que tenga en la computadora incluyendo todos los archivos y cualquier ***software*** que haya instalado.

Notas

Seguridad *en* Cibernética

Capítulo 2



Una guía de protección para el consumidor en el mundo cibernético

ANUNCIOS, APLICACIONES Y SEGURIDAD PERSONAL

El problema: Confusas, engañosas o falta de políticas de privacidad

Anuncios en línea: Un negocio de billones. Las computadoras tienen la capacidad de recoger una gran cantidad de información acerca de usted, y de transmitirla a terceras partes incluyendo los comerciantes y las redes de publicidad.

La industria americana de publicidad en línea generó $31.7 billones de ingresos en el 2011, un incremento del 22 por ciento de los años anteriores, según reportes en los medios de comunicación. Este mega negocio, muy competitivo, está fomentado en mayor parte por la venta y compra de información personal como los gustos y características del usuario de internet.

Las compañías de publicidad quieren aprender todo lo que pueden acerca de usted, para crear anuncios diseñados especialmente para incitarlo a comprar lo que venden. Esta información la obtienen de varias maneras: contratan con distintos sitios de comunicación de redes sociales, ponen ***"cookies"*** –pequeños archivadores de texto- en su navegador para rastrear lo que mira en la web y por cuanto tiempo está en ella, o contratan con los fabricantes de los programas de teléfonos inteligentes- que pueden incluso usar un Global Position System

o **GPS** (Sistema de Posición en el Globo) para reportar donde está localizado. Usted tiene el derecho de proteger su privacidad optando por salirse de los sistemas de rastreo. Puede hacerlo manejando sus configuraciones de privacidad en las cuentas de su red social, en sus navegadores de la red y en sus teléfonos inteligentes y otros aparatos.

Anuncios Personalizados para el usuario. Los "anuncios personalizados" lo que se llama en inglés ***"behavioral advertising"*** envuelve la recolección de información de su actividad en línea, y usarla para bombardearlo con anuncios a sus aparentes gustos. Las compañías que se envuelven en esta clase de práctica de publicidad, recogen la información sin que usted lo sepa. Por ejemplo si usted navega por un sitio web que vende ciertos automóviles, el ***cookie*** puede hacer una nota de lo que le interesa y le mandará anuncios de autos vendidos en ese sitio web, esto se llama ***first-party behavioral advertising.*** Otras veces las compañías de publicidad se envuelven en rastrear sus actividades en varios sitios webs ***(third-party)***, y le mandará anuncios de todos los sitios que ha visitado. Muchos de los cookies colocados por las compañías de third-party continúan rastreando sus actividades incluso después que usted ha dejado el sitio web.

Navegadores de la red y configuraciones de privacidad. Muchos navegadores de internet tienen configuraciones que les dice a los sitios webs que no pongan ***third-party cookies*** en sus computadoras - y por lo tanto no pueden rastrear sus actividades de un sitio web a otro. Este capítulo concluye con información de cómo puede ajustar las configuraciones de privacidad en sus navegadores de la red que usted usa. Pero como hemos indicado varias veces en este capítulo, las configuraciones para proteger su privacidad pueden ser manipuladas.

La Federal Trade Commission o **FTC** (Comisión Federal de Comercio) en Agosto del 2012 anunció un acuerdo de $22.5 millones con **Google**, debido a acusaciones que **Google** engañó a los consumidores acerca del seguro de privacidad en relación a los ***cookies*** y **web browsers** (navegadores de la red). Según la FTC, Google engañó a los usuarios de navegadores de la red de Safari, diciéndoles que las configuraciones de privacidad de Safari bloquearían a los ***third-party cookies.*** La FTC alegó que, a pesar de hacer estas promesas, Google evadió la configuración de los navegadores de la red de Safari y puso cookies rastreadores en las computadoras de los usuarios por varios meses en los años 2011 y 2012.

Teléfonos inteligentes: "sus aplicaciones lo están vigilando"- Pocos aparatos saben tanto acerca de usted como su teléfono inteligente o su computadora móvil ***(tablet pc)***. Aparatos como el **iPhone**, **iPad**, y el teléfono **Android** son capaces de rastrear sus actividades en línea y mucho más. Estos pueden incluir un GPS que sabe dónde está el aparato, o un aparato especial de identificación ***(Unique Device Identifier or UDID)*** que nunca se puede desactivar.

El lanzamiento del iPhone en el 2007 creó un mercado de billones de dólares de aplicaciones móviles, o ***apps*** -juegos y otros programas disponibles para usarlos en los aparatos móviles. Hoy, más de 500,000 apps están disponibles en la **Apple App Store** y otras 480,000 en el **Android Market.** Han sido descargadas 28 billones de veces por cientos de miles de usuarios, según un sondeo de la FTC. Un observador llamó a las ***apps*** "el futuro del mercado digital" porque se usan para todo desde "ver cines a pedidos de comidas"

Una gran cantidad de **apps** educacionales y de entretenimiento se han mercadeado especialmente para niños. Más de un cuarto de todos los padres han descargado apps para que sus hijos los usen, según un estudio del **Joan Ganz Cooney Center del Sesame Workshop en el 2012.**

Sin embargo muchas de las ***apps*** han transmitido información de sus usuarios a otros. Un estudio de 101 ***apps*** del **Wall Street Journal** en el 2010, publicado con el título **"Sus *apps* lo están vigilando"**, descubrió que 56 de las apps transmitieron el identificador UDID a partes terceras, 47 transmitieron el lugar del teléfono, y 5 mandaron la edad, sexo, y otros detalles personales a extraños. La FTC reportó en Febrero del 2012 que la mayoría de las ***apps*** mercadeadas para los niños no tienen las adecuadas declaraciones de privacidad, que ayudaría a los padres saber si están recogiendo o transmitiendo información personal.

La **División de Asuntos del Consumidor de Nueva Jersey** en Junio del 2012 demandó a un programador de California de unas de las ***apps*** educacionales más vendidas y populares para niños preescolares y hasta segundo grado. Los investigadores de la División descubrieron que las ***apps*** habían transmitido información personal –incluyendo el nombre y apellido de los usuarios así como los UDID de los teléfonos a una tercera parte, una compañía de análisis de información.

La compañía recogió y transmitió la información sin proveer notificación en su sitio web y **sin obtener un permiso verificado de los padres.** La demanda fue la primera puesta en Nueva

Jersey bajo la ley federal **Children Online Privacy Protection Act** (Acta de Protección de la Privacidad de Niños en Línea). En el convenio el programador de las ***apps*** acordó a parar de recoger información sin el consentimiento de los padres, y asegurar que iba a destruir la información previa que fue transmitida.

Los padres tienen que estar alerta ya que algunas de las ***apps*** tienen un mecanismo construido dentro que les permite a los usuarios hacer compras mientras están interactuando con otra ***app*** (por ejemplo, permiten al usuario comprar historias adicionales cuando están usando un ***app*** de un libro de historias). Algunas ***apps*** también pueden estar integradas con redes sociales como **Facebook** o **Twitter**. Estas ***apps*** se pueden mercadear sin información que pueden alertar a los padres de estas posibilidades, según el estudio de la FTC, titulado **"Mobile Apps for Kids: Current Privacy Disclosures are Disappointing"** (***Apps*** móviles para niños: las actuales declaraciones de privacidad son decepcionantes.)

Socialización en la red: ¿está su vida expuesta en línea? Facebook, MySpace, y otros sitios webs de redes sociales han transformado la manera como millones de gente se conectan e intercambian información. Han emergido como un nuevo medio poderoso- pero también

como una fuente importante de información para los comerciantes. El gobierno del Estado de Nueva Jersey usa **Facebook** y **Twitter** para comunicarse con el público, y la **División de Asuntos del Consumidor** mantiene una página web en **Facebook**.

Facebook tiene más de 955 millones de usuarios activos; **Twitter** tiene más de 500 millones; **Google+** tiene más de 250 millones de usuarios registrados; **LinkedIn** tiene más de 175 millones; y **MySpace** reportó 25 millones solamente de EE.UU. en Junio del 2012. Sin embargo, usted debe usar estos sitios a su propio riesgo-y el riesgo de exponer su información personal al resto del mundo. **Nada en línea es privado.** Incluso las más férreas configuraciones de seguro de privacidad no cambian el hecho de que cualquier cosa que ponga en línea – o mande a través de un **"seguro" mensaje de chateo –puede copiarse y compartirse con otros.**

En Diciembre del 2009, la FTC acusó a Facebook de engañar a los usuarios por decirles que ellos podían mantener su información privada – y luego repetidamente permitir que ésta fuera compartida y hecha pública. Entre otros cargos, la FTC argumentó que Facebook compartió información personal con los comerciantes, después de prometer que no lo haría. En Agosto del 2012 en el acuerdo final con la FTC, Facebook acordó a darle a los consumidores noticia

clara y obtener su permiso explícito antes de compartir la información, y hacer cada dos años una auditoría de asuntos de privacidad.

La FTC acusó a **Google** de engañar a los consumidores y violar sus promesas de privacidad cuando lanzó su primera red social, llamada **Google Buzz**, en el 2010. **Google** lanzó la red social a través de Gmail su sistema de email en la red. La FTC alegó que **Google** hizo creer a los usuarios de Gmail que ellos podían escoger si querían pertenecer a la red Buzz, pero las opciones de declinar o dejar la red social fueron ineficaces; y para aquellos que decidieron pertenecer, los controles para limitar y compartir su información personal eran confusos y difíciles de encontrar. En su acuerdo final en Octubre del 2011 con la FTC, **Google** acordó a implementar un programa exhaustivo de privacidad así como auditorías independientes de privacidad por los próximos 20 años.

Es muy fácil compartir demasiada información en la red. La mayoría de las redes sociales le piden que haga un perfil personal con información detallada. Le pueden preguntar por su actual y previos lugares de trabajo, su formación educacional, la ciudad donde reside, e incluso su email, su número de teléfono celular, y su identificador de mensajes instantáneos.

Toda esta información lo puede exponer a robo de identidad o ataques de ingeniería social, como fue descrito en el Capítulo 1 de este manual.

Como veremos en el capítulo 3, predadores han usado información personal de sus víctimas para tomar posesión de los emails o de las cuentas de las redes sociales. Para abrir una cuenta de internet, la mayoría de los sitios webs con los cuales hace negocio le preguntarán detalles de seguridad como: **"¿Cuál era el nombre de su primera mascota?" "¿Cuál es el apellido de su madre?" "¿Cuál fue la calle donde se crió?"** para que en caso de que haya olvidado su contraseña, respuestas a estas preguntas confirmarán su identidad. **Si pone demasiada información en línea los piratas de cibernética la pueden usar para acertarlas.**

Antes de poner información en línea, considere que mucha información en su perfil público puede exponer sus creencias religiosas y políticas, sus relaciones, u otra información confidencial a partes terceras como a sus empleadores actuales o potenciales, escuelas, amigos, conocidos o competidores comerciales. **Información indiscriminada pública puede dañar su reputación, carrera, sus perspectivas educacionales, y relaciones personales.**

Los legisladores de Nueva Jersey han propuesto leyes que van a prohibir que los

empleadores requieran de los empleados o de los que estén solicitando trabajo, las contraseñas del perfil de sus redes sociales. Como veremos en el capítulo 3, revelar mucha información acerca de sus actividades diarias puede ponerlo en peligro, o que invite a ladrones a su casa si ha puesto en Facebook que se va de vacaciones.

Muchos sitios de socialización en la red permiten que otra gente comparta información acerca de usted –como sus fotos o videos- que puede ser que usted prefiere mantenerlos privados. Estos sitios webs por lo general incluyen configuraciones que le dan cierto control de privacidad acerca de quién puede ver lo que usted ha puesto en la red, quién lo puede "tag", y quién puede ver los artículos en los que usted está.

Sin embargo, **incluso las mejores y más claras configuraciones de seguridad no cambian la posibilidad de que todo lo que pone en una red social pueda hacerse público-lo mismo que un email que usted mande solamente a una persona, ésta lo puede hacer público para que todo el mundo lo vea.**

La solución: Tome control de su privacidad. Sitios webs de socialización en la red: use sentido común. Algunos usuarios de internet comparten información personal en la red que no harían con los extraños de la calle. Incluso con las mejores configuraciones de privacidad, debe pensar que cualquier cosa que ponga en la red será compartida y vista por otros.

Use sentido común a todo tiempo cuando ponga información en línea- incluso cuando provea detalles de su perfil de usuario, tuiteando, actualizando su información, blogueando, o incluso cuando manda un email a una sola persona.

A veces nos dejamos llevar por un momento de euforia. Lo mejor es pararse, pensar y considerar lo que se va a poner. ¿Cómo se sentiría si lo que ha puesto lo viera su empleador, o sus futuros empleadores, su entrenador o maestros, sus padres, hijos, o amistades? También debe considerar la privacidad de otros, especialmente cuando pone una foto, video, o comenta acerca de un amigo o pariente.

Recuerde que incluso cuando borra algo que usted puso, estará todavía en los servicios de la red y asequible a motores de búsqueda.

Socialización en la red: evalúe sus configuraciones de privacidad. Tómese tiempo para comprobar las configuraciones y la política de privacidad de todas sus redes de socialización, blogs, y otras vías en las que usted haya puesto su perfil o información personal. Si no encuentra las configuraciones de privacidad, póngase en contacto con el editor de su sitio web y pregunte por esta información.

Después de ajustar sus configuraciones de privacidad, debe chequear estas con frecuencia. Es importante recordar que muchas de las redes de socialización cambian sus configuraciones y políticas en el curso de los años. So tenga en cuenta que esas políticas pueden cambiar otra vez.

Socialización en la red: defiéndase de *phishing* y *malware*. Cómo se ha anotado previamente, algunos mensajes que puede recibir en los sitios de socialización pueden ser en actualidad ***phishing*** o ***Trojan horses.***

Tiene que tener cuidado con las aplicaciones de partes terceras como juegos, encuestas, concursos y cuestionarios que se encuentre en las redes sociales. Usando estas aplicaciones puede exponer su computadora a códigos maliciosos o su información personal a publicidad no deseada.

Protéjase siguiendo los pasos descritos en las páginas 10 hasta la 18. Proteja su computadora manteniendo sus programas de software actualizados. Proteja su perfil usando contraseñas 'inteligentes', y siempre verifique la autenticidad de un mensaje antes de pulsar en él.

Como bloquear los cookies de publicidad- Protéjase: chequee su navegador de red. Cuando use un navegador de red, es una buena idea chequear las configuraciones de privacidad de éste. También considere si quiere borrar a mano y regularmente, los cookies que hayan puesto en su computadora. Vaya a la página 13 hasta la 15 para información adicional.

Para información de cómo ajustar las configuraciones de seguridad de su navegador en la web, visite el sitio web del vendedor de su navegador, o póngase en contacto con éste para preguntar por las instrucciones.

Mantenga un ojo en las aplicaciones de su teléfono inteligente- Como se ha anotado arriba, muchas de las aplicaciones de los teléfonos inteligentes coleccionan información personal y la mandan a partes terceras, o permite a los usuarios a interactuar con los sitios de socialización de la red. Los padres tienen que comunicarse con sus hijos para saber qué clase de juegos y apps de educación usan en estos teléfonos. Vea "La solución: Comuníquese y empodere a su familia" en la página 41.

Capítulo 3

Seguridad en Cibernética

Una guía de protección para el consumidor en el mundo cibernético

El problema: predadores, intimidadores y contenido inapropiado
Acecho en cibernética, Asalto Sexual y Extorsión Sexual

Un hombre de Perth Amboy admitió culpabilidad en Agosto del 2012 después de haber violado a dos adolescentes que había acechado en el internet. El hombre de 29 años de edad creó un perfil usando un nombre falso, pretendiendo que tenía 17 años. Él se hizo amigo de dos adolescentes de 14 años, y empezó a mandarles mensajes sexuales explícitos.

Una de las adolescentes lo conoció en persona. La otra rehusó sus insinuaciones sexuales –pero **el predador leyendo todo lo que la adolescente ponía en Facebook pudo localizarla y encontrar su paradero. Ambas adolescentes fueron violadas.**

Él usó las mismas artimañas de los depravadores sexuales de internet: observando lo puesto en línea por las víctimas, aprendió dónde y cuándo éstas iban a estar; se hizo amigo de las adolescentes con una identidad falsa; gradualmente y amistosamente las coaccionó, luego coqueteó con ellas, y finalmente terminó con mensajes sexuales explícitos.

Según reportes en los medios de comunicación, uno de los más notables casos de cyberacecho de la última década fue el de Jonathan Vance, quién se escondió detrás del nombre de Metascape. Él intentó usurpar más de 200 cuentas de Facebook, MySpace, y emails de adolescentes y mujeres jóvenes entre los 14 y 26 años, y **aterrorizó por lo menos a 53 para que le mandaran fotos sexuales de ellas.**

Él usó diferentes métodos para acceder a las cuentas en línea de las víctimas. En muchos de los casos, la información la encontró en las redes de socialización y en línea, como cumpleaños, nombres de las escuelas, y pueblos. Cómo se ha explicado antes, él fue a las cuentas de las jóvenes y pulsó en: **¿Se le olvidó la contraseña?**, y usó la información encontrada en las redes sociales para acertar las preguntas de seguridad.

En otras ocasiones, él se puso en contacto con sus víctimas a través de mensajes instantáneos. Pretendiendo ser una amiga o pariente, decía que había sido bloqueado de su cuenta en línea, y les pedía si podían "prestarle" la contraseña de sus cuentas de Facebook, MySpace o email.

En todos los casos una vez que Vance tenía acceso a las cuentas en línea de las víctimas, inmediatamente cambiaba las contraseñas –tomando control completo de las cuentas. Luego amenazaba a las jóvenes que las iba a humillar haciendo público secretos vergonzosos y otra información, si no le mandaban fotos desnudas de ellas. En Abril del 2009, Vance fue sentenciado a 18 años en la prisión federal.

El **Crimes Against Children Research Center** (Centro de Indagación de Crímenes en contra de Niños) de la Universidad de New Hampshire (EE.UU.) reportó en Diciembre del 2011 que el porcentaje de jóvenes que recibieron mensajes sexuales en el internet sin haberlos solicitado, declinó de un 13 por ciento en el 2005 a un 9 por ciento en el 2010 -y anotó que más información en los medios de comunicación acerca del problema podía haber contribuido a la reducción.

Acosadores en cibernética (cyberbullies): crueldad a larga distancia-Acosadores usan computadoras, teléfonos celulares y aparatos móviles para acosar, amenazar, humillar, o atormentar a otros. Esto lo pueden hacer a través de crueles mensajes de textos o divulgando rumores acerca de las víctimas en teléfonos celulares o en línea.

Adolescentes han creado páginas webs para burlarse de sus amigos; y han fabricado falsos humillantes perfiles de los que quieren intimidar en sitios de redes sociales. Los acosadores han usado aparatos móviles para tomar fotos o videos vergonzosos y luego los han puesto en el internet para que todo el mundo los vea y comente en ellos.

Algunos intimidadores encuentran que es más fácil para ellos ser crueles en línea porque no hay confrontación personal. Las víctimas se creen que todo el mundo sabe de sus humillaciones, de los insultos y de las fotos y que todos las ridiculizan; y la avalancha de emails acosadores y de mensajes de texto las hace sentirse atrapadas. Las consecuencias emocionales para las víctimas son devastadoras.

Ha habido casos notorios donde las adolescentes víctimas se han suicidado, y en parte se cree que el hecho de ser una víctima de cyberbullies precipitó el suicidio. El **Cyberbullying Research Center** (Centro de Indagación de Acoso en Cibernética), anotó que todas las formas de acoso están conectadas con un aumento de contemplación de suicidio, y que las víctimas de cyberbullying eran casi dos veces más propensas a intentar suicidarse que aquellas que no lo eran.

Aproximadamente el 20 por ciento de estudiantes entre los 11 y 18 años de edad indicaron que habían sido víctimas de cyberbullying, según el **Cyberbullying Research Center.** El Crimes Against Children Research Center descubrió que el acoso en línea parece que está incrementando para la juventud, especialmente para niñas.

Sexting: Posibles consecuencias para toda una vida- *Sexting:* la transmisión de fotos de personas desnudas o en posiciones sugestivas sexuales- puede tener una repercusión de serias consecuencias. Cerca del 4 por ciento de jóvenes entre los 12 y 17 años que tienen teléfonos celulares han mandado fotos sexuales sugestivas de ellos a otros, y el 15 por ciento ha recibido dichas imágenes.

Adolescentes que han mandado fotos de ellos o de otros, han sido cargados con distribución de pornografía infantil porque están mandando fotos de menores desnudos, e individuos que han recibido estas fotos han sido cargados con posesión de esta pornografía. **Los que quebrantan esta ley pueden terminar en el registro de ofensores sexuales de su estado.**

Una joven de 18 años del Estado de Ohio mandó fotos de ella desnuda a su novio –y éste las circuló

entre otros después que rompieron sus relaciones, lo que causó una extensiva e incesante humillación verbal y abuso a la muchacha en la escuela. Dos años después la chica terminó suicidándose.

Otras maneras de chatear con extraños-El internet ofrece una variedad sin fin a los usuarios para que puedan conectarse con extraños, y muchas maneras en las que los niños pueden estar expuestos a predadores o a contenido inapropiado.

Apps* de teléfonos móviles:** *Apps* móviles, y sus capacidades de GPS, traen el riesgo de conectarse con extraños en un nivel nuevo. **Skout**, una ***app de coqueteo, permite que los usuarios encuentren y se pongan en contacto con otros usuarios cercanos. Sus dueños suspendieron el servicio para menores en Junio del 2012, después que en tres incidentes separados, **adultos pretendiendo ser adolescentes, se pusieron en contacto con niños a través de Skout y los asaltaron sexualmente.** Las víctimas fueron dos niñas de 12 y 15 años, y un niño de 13 años, según fue reportado en los medios de comunicación.

Consolas de Juegos de Videos: muchas consolas de juegos de videos –como **Xbox de Microsoft, PlayStation de Sony, y Wii de Nintendo** –ofrecen a los usuarios la posibilidad de navegar en el internet, mandar y recibir fotos y mensajes, y competir con jugadores de todo el mundo.

Predadores sexuales de niños han hecho los **juegos de videos** el blanco de sus búsquedas porque es fácil encontrarlos allí– y muchos de ellos **ven esto como la manera perfecta dónde pueden hacer que los niños se encuentren completamente a gusto con un extraño.** Para preparar a la inocente víctima, empiezan comunicándose con ésta a través de los juegos, luego desarrollan una "amistad" y finalmente la incitan a un encuentro.

Sitios web de chateo anónimos: Chatroulette y Omegle ambos creados por adolescentes, son sitios de chateo en línea que conectan adolescentes por videos o conversaciones de texto. Un sondeo del 2010 conducido por la compañía RJMetrics, descubrió que uno de ocho videos emparejados en Chatroulette produjo "algo clasificado para mayores (R-rated) o peor", aunque ahora Chatroulette marca a los usuarios que transmiten contenido sexual.

La solución: Comuníquese y empodere a su familia- Las siguientes sugerencias están adoptadas de las que ofrece el **National Center for Missing and Exploited Children o NCMEC** (Centro Nacional de Niños Desaparecidos y Explotados) y sus recursos de **NetSmartz.**

Imponga reglas, y limite el tiempo que sus hijos pasan en línea- Ponga reglas sencillas, claras, y fáciles de entender indicando cuándo y dónde usted permitirá que sus hijos

usen el internet en su casa y de vez en cuando revise las reglas con sus hijos. Limite los sitios webs a los que sus hijos puedan acceder, y cuándo puedan ir a estos. Ejemplos de reglas se pueden encontrar en: **www.NetSmartz411.org** (hay información en español).

Dígale a sus hijos que no den información personal o de la familia, o que pongan fotos o videos a no ser que usted ha revisado los materiales y le ha dado permiso para hacerlo. Hágales saber de todos los peligros que se han expuesto en este manual acerca de los estafadores, piratas de cibernética y predadores.

Computadoras, videos, juegos y otros aparatos con los que puedan acceder al internet, deben tenerse en la sala de estar, o en un sitio semejante donde un adulto puede supervisarlos. Aprenda de otros sitios donde sus hijos pueden tener acceso al internet, como en casa de sus amigos, librerías o escuelas. Tenga un plan para poder monitorear a sus hijos cada vez que vayan en línea.

Considere darles a sus hijos un teléfono celular con acceso limitado al internet, en vez de un teléfono inteligente. Hable con los fabricantes o los vendedores de los teléfonos para saber sus opciones. ¿Qué hacer si usted es un padre que no es familiar con computadoras o el internet? El National **Center for Missing and Exploited Children** ofrece **www.NetSamrtz411.org** un recurso para

padres y guardianes acerca de la seguridad en la computadora; los expertos de NetSmartz proveen respuestas directas por teléfono en **888-NETS411 (888-638-7411)**. NCMEC también provee **www.NetSamrtz.org** con videos y tutoriales para padres, educadores, adolescentes y niños.

Siéntese con sus hijos para hablar de los riesgos del internet y de los beneficios y de las actividades de diversión que pueden disfrutar si usan el internet de una manera responsable. Vayan al internet juntos, y deje que ellos les enseñen los sitios que están visitando y de qué manera lo están usando; esto puede ser una manera de interactuar con sus hijos además de una actividad agradable

Para bloquear pornografía y otros materiales cuestionables, considere comprar programas de software de filtro y de monitoreo de internet. Los filtros restringen acceso a ciertas clases de sitios webs y pueden limitar el tiempo que los niños pasan en línea. Monitoreando los programas de software le permite rastrear las actividades de otra persona en una computadora. Recuerde que estas herramientas no son infalibles, y no son una substitución adecuada de supervisión paternal.

Recuerde a sus hijos que no hablen con extraños –y que le digan, sin temor, si alguien en el internet que no conocen se quiere comunicar con ellos.

Las mismas reglas que se aplican en la vida diaria se aplican en línea. Además de los sitios de NetSmart mencionados arriba el **National Center for Missing and Exploited Children** provee información importante en **www.MissingKids.com** , incluyendo la serie "Sepa las reglas" de las varias maneras de cómo proteger a los niños.

Si su niño le dice que alguien que ha conocido en línea quiere "conocerlo" en persona, elógielo por habérselo dicho; esto ayudará a mantener abiertas las líneas de comunicación. Si sospecha que la persona es un adulto intentando citarse con un niño, póngase en contacto con la policía –y ponga un **CyberTipline** reporte con NCMEC en **www.CyberTipline.com** o llame al **800-843-5678.** Si es otro niño, hable con los padres o guardianes de éste. Si todos están de acuerdo con la visita, acompañe a su niño para conocer al joven y a los padres, y arregle la cita en un sitio público.

Aviso para adultos que quieran citarse en línea: nunca dé su dirección u otra información personal a alguien que no conoce. Si decide ponerse en contacto con la persona con la que se está correspondiendo, hágalo en un sitio público, y dígale a un amigo o a su familia dónde va a estar y con quien se va a citar.

Sexting y cyberbullying- Hable con sus hijos acerca de las posibles consecuencias de mandar in-

apropiadas fotos a amigos u otros. Chequee la computadora y el teléfono celular de sus niños para ver si hay fotos que puedan ser mal interpretadas por otros si las ven. Si ve fotos inapropiadas, prohíba el acceso al internet y quítele las cámaras digitales. También encuentre a quien le mandaron las fotos. Póngase en contacto con **CyberTipline**, si descubre que fotos de contenido sexual explícito de sus niños están circulando el internet. Llame a la policía e informe a su ISP si es necesario.

Si sus hijos están recibiendo emails, mensajes instantáneos, o alguien está poniendo comentarios en la red acerca de ellos, **asegúrese que no respondan.** Haga copia de la información en caso que la tenga que tener de prueba. Cierre la cuenta de internet y abra una nueva. Dé el email nuevo solamente a unas pocas personas en las que confíe completamente. Ayude a sus hijos bloquear mensajes instantáneos o emails de los números o cuentas de aquellos que están mandando los mensajes ofensivos. Si un acosador de internet ha abierto un sitio web para difamar o burlarse de su hijo, póngase en contacto con su ISP, o el administrador del sitio web inmediatamente. **Si es necesario, informe a la policía para que remuevan el sitio web.**

Envuelva a la escuela. Aprenda la política de la escuela acerca de ***cyberbullying***, y urja a los administradores **que tomen una posición en contra del acoso en el internet.**

APPÉNDICE I: Si cree que ha sido víctima de robo de identidad…

INMEDIATAMENTE reporte el incidente de robo de identidad a una agencia de implementación de leyes, como por ejemplo la policía local, o la Oficina del Procurador de su Condado donde el robo tuvo lugar. Obtenga una copia del reporte para que pueda mandarla a las agencias de reporte de crédito y a los acreedores.

Ponga una queja con la Comisión Federal de Comercio a **www.ftc.gov/complaint o llame al 1-877-438-4338**; TTY (telecomunicación para sordo-mudos) al 1-866-653-4261. Su queja completa se llama un "FTC Afidávit". Lleve su Afidávit a su policía local donde el robo ocurrió y donde puso el reporte.

Obtenga un acopia de reporte de crédito de las tres agencias de crédito yendo a:

Equifax Credit Information Services-Consumer Fraud Division
P.O. Box 740250
Atlanta, GA 303748
Teléfono: 800-525-6285 • www.equifax.com

Experian
P.O. Box 1017
Allen, TX 75013-2104
Teléfono: 888-397-3742 (888) 397-3742 • www.experian.com/consumer
Facsimile: 800-301-7196 (fax)

Trans Union
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92634
Teléfono: 800-680-7289 • www.tuc.com

Asistencia adicional para poder obtener los reportes de crédito se pueden encontrar llamando al número: 1-800-242-5846 o yendo a: www.njconsumeraffairs.gov/espanol/spbrief/credit.pdf

Reporte a todas las agencias mencionadas si alguien le ha robado las tarjetas de crédito o los números de las tarjetas de crédito, y pida que todas sus cuentas se marquen con una alerta de fraude de crédito.

Póngase en contacto con todas las compañías de crédito, sus acreedores, bancos e instituciones financieras con las cuales tiene una relación comercial. Cierre las cuentas que cree han sido afectadas por el robo de identidad, y reemplace sus tarjetas de crédito con otras nuevas. Cambie su contraseña en todas sus cuentas, incluyendo su **PIN** (Número Personal de Identificación). Siga todas sus conversaciones por teléfonos con una confirmación escrita.

Póngase en contacto con la Administración del Seguro Social de los EE. UU. , yendo a:

Social Security Administration, Fraud Hotline
Office of the Inspector General
P.O. Box 17768
Baltimore, MD 21235
Teléfono: 800-269-0271
Facsímile: 410-597-0018
www.ssa.gov/oig/hotline • oig.hotline@ssa.gov

Haga un archivo con toda la información relacionada al robo de identidad: mantenga notas escritas de todas sus conversaciones, con las direcciones y teléfonos de todos sus acreedores, agencias de reporte de crédito y agencias de colección de débito. Guarde copias de toda la correspondencia mandada y recibida. Mándelo todo por correo certificado, con recibo de retorno. Guarde todos los recibos de todos los gastos relacionados con el robo de identidad, y el tiempo gastado en el problema, en caso que demande restitución en un juicio o convicción en contra del ladrón.

Puede también ponerse en contacto con agencias sin fines de lucro establecidas para asistir a víctimas de robo de identidad. Como:

Privacy Rights Clearinghouse
Identity Theft Resource Center
3108 Fifth Avenue, Suite A
San Diego, California 92103
Teléfono: 858-693-7935
www.privacyrights.org • www.idtheftcenter.org

APENDIX II: Recursos adicionales

El **United States Computer Emergency Readiness Team o US-CERT** (Equipo de Preparación de Emergencia de Informática de los Estados Unidos), dentro del **U.S. Department of Homeland Security** (Departamento de Seguridad Nacional de Estados Unidos) proveyó las sugerencias del primer capítulo de este manual. Para más información vaya a: **www.US-CERT.gov**.

La **Federal Trade Commission** o FTC (Comisión Federal de Comercio) provee información importante acerca de la seguridad en cibernética si va a: **www.consumidor.ftc.gov/**.

El **National Center for Missing and Exploited Children** o NCMEC (Centro Nacional de Niños Desaparecidos y Explotados) y sus recursos de **www.NetSmartz.org** ofrece información importante acerca de seguridad en el internet, para padres si va al: **www.NetSmartz411.org** con expertos preparados para contestar sus preguntas en: **888-NETS411 (888-638-7411)**; y para los adolescentes y niños si va a: **www.NetSmartz.org**.

Información adicional acerca de cyberbullying y sexting **Cyberbullying Research Center** (Centro de Indagación de Acoso en Cibernética), yendo a: **www.cyberbulying.us**.

Para más información al día en estos asuntos y otros, chequee **Consumer Alerts** (Alertas a Consumidores) en el sitio web de la División **www.NJConsumerAffairs.gov**, síganos en Facebook, y vea el calendario de la interacción de la División con la comunidad en: **www.NJConsumerAffairs.gov/outreach**.

Notas

Notas

Manual de Seguridad en Cibernética

Manual de Seguridad en Cibernética

www.NJConsumerAffairs.gov ■ 1-888-656-6225

2013